

- 7 -

REMARKS

The Examiner has rejected Claims 1-6, 8-16 and 19-21 under 35 U.S.C. 102(e) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457). In addition, the Examiner has rejected Claims 28-30 under 35 U.S.C. 102(e) as being anticipated by Dondeti et al. (U.S. Patent No. 6,240,188). Further, the Examiner has rejected Claims 38 and 39 under 35 U.S.C. 102(e) as being anticipated by Kandansky et al. (U.S. Patent No. 6,295,361). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to substantially incorporate the subject matter of either dependent Claim 10 or 16.

With respect to the subject matter of Claim 10, as incorporated into some of the independent claims, the Examiner has relied on the following excerpts from Gundavelli to make a prior art showing of applicant's claimed technique "wherein said updating does not use new secret information" (see the same or similar, but not necessarily identical language in all but one of the independent claims).

"According to another aspect, upon determining that a first departing member has left the second multicast group a private multicast group non-zero random integer is selected. A second multicast group exchange key is then generated based on a private multicast group non-zero random integer, a public non-zero integer and a public prime integer. The second multicast group exchange key is then broadcast to each remaining member of the second multicast group for computing a third secret key that is based on the second multicast group exchange key and the second shared secret key. Through the use of the third shared secret key a third multicast group is established whose members include only remaining members of the second multicast group as the third shared secret key provides a second secure channel for communicating between members of the third multicast group over the insecure network." (Col. 5, lines 47-63-emphasis added)

"Although the examples provided herein illustrate adding users to a multicast group dynamically, the techniques described are also applicable to multicast groups in which members are deleted dynamically. For example, the multicast group may desire to exclude a member who has left the group from future communications between the remaining members. In certain embodiments, when a member leaves the multicast group, a new

- 8 -

shared secret key is generated for communicating between those members that remain in the multicast group. Using the new shared secret key, the members remaining in the multicast group can communicate over a secure channel and the departed member cannot decrypt the communications.

In one embodiment, when a person leaves the group, a new shared secret key is established using the traditional Diffie-Hellman algorithm. The remaining members may then use the newly established shared secret key to securely communicate with each other. In addition, the new members may be admitted into the group using the method described above.

For example, referring to FIG. 3E, if Carol 314 leaves the multicast group 328, the remaining members within multicast group 330 may establish a new secret key using the traditional Diffie-Hellman algorithm. In addition, the multicast group 330 may compute a multicast group 330 exchange key for admitting new members into the multicast group 330. For example, upon Carol 314 leaving multicast group 328, multicast group 330 may communicate with each other to compute a new shared secret key  $k_4$  using the traditional Diffie-Hellman algorithm. In addition, the multicast group 330 may compute an exchange key  $K_3'$  as previously explained above, for admitting new members into the multicast group 330. For example, the exchange key  $K_3'$  may be computed as  $K_3' = (gk_4 \text{ mod } (n)).$ " (Col. 11, lines 6-39)

Applicant respectfully asserts that above excerpts cited by the Examiner actually *teach away* from applicant's specific claim language. In particular, Gundavelli discloses that "upon determining that a first departing member has left the second multicast group a private multicast group non-zero random integer is selected. A second multicast group exchange key is then generated based on a private multicast group non-zero random integer, a public non-zero integer and a public prime integer" (see emphasized except above).

Thus, in Gundavelli when a member has left a group, new secret information is utilized in creating the exchange key, including "a private multicast group non-zero random integer, a public non-zero integer and a public prime integer," as expressly disclosed. Applicant, on the other hand, claims that the "updating does not use new secret information" (emphasis added).

With respect to the subject matter of Claim 16, as incorporated into of the remaining independent claim, the Examiner has again relied on the above cited

- 9 -

excerpt to make a prior art showing of applicant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key."

Applicant respectfully asserts that simply nowhere in Gundavelli is there any disclosure that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by applicant. In fact, applicant notes that such excerpts only disclose utilizing random integers to create an updated key (see emphasized excerpt above) and using the traditional Diffie-Hellman algorithm to create a new shared secret key. Clearly, such teachings do not even suggest that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the respective references, especially in view of the amendments made hereinabove. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 7, as rejected under 35 U.S.C. 103(a) as being unpatentable over Gundavelli in view of Takeda (U.S. Patent No. 6,178,244), the Examiner has relied on Col. 12, lines 38-43 in

- 10 -

Takeda to make a prior art showing of applicant's claimed technique "wherein said updating occurs on a periodic basis." Applicant respectfully asserts that such excerpt relied on by the Examiner does not teach that updating at least one compromised secret "on a periodic basis" in the context claimed by applicant. Instead, Takeda only discloses updating a session key in response to certain circumstances, namely right after receiving the session key, when the communication is interrupted, and when a predetermined time period has passed after receiving the session key. Clearly, such circumstances do not meet applicant's claimed periodic basis.

Applicant respectfully asserts that the references relied on by the Examiner do not teach or even suggest all of applicant's claim limitations. Thus, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 40-41 below, which are added for full consideration:

"wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user" (see Claim 40); and

"wherein a single non-compromised secret is utilized to update a plurality of compromised secrets by using a one-way function with inputs of said single non-compromised secret and said non-compromised secret" (see Claim 41).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees

- 11 -

are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P089/00.175.01).

Respectfully submitted,

  
Kevin J. Zilka  
Registration No. 41,429

P.O. Box 721120  
San Jose, CA 95172  
Telephone: (408) 505-5100